



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya WebLM License Manager for Avaya VPNremote™ Phone Release 2 – Issue 1.0

Abstract

These Application Notes describe the steps for configuring the Avaya WebLM License Manager to support Avaya VPNremote™ Phones.

Avaya WebLM is a Web-based license manager application designed to support Avaya software products that require licensing. The Avaya VPNremote™ Phone is a software based Virtual Private Network (VPN) client integrated into the firmware of an Avaya IP Telephone. Release 2 of the Avaya VPNremote Phone utilizes Avaya's WebLM license management system. The Avaya VPNremote Phone license file must be installed on the WebLM server for the Avaya VPNremote Phone to be fully functional. A WebLM client integrated into the Avaya VPNremote Phone communicates with the WebLM sever for license verification during the phone startup process.

TABLE OF CONTENTS

1. INTRODUCTION.....	3
1.1. VPNREMOTE PHONE STARTUP	4
2. NETWORK TOPOLOGY	5
3. EQUIPMENT AND SOFTWARE VALIDATED.....	6
4. AVAYA VPNREMOTE PHONE CONFIGURATION.....	6
4.1. VPNREMOTE PHONE FIRMWARE.....	6
4.2. CONFIGURING AVAYA VPNREMOTE PHONE	7
5. AVAYA WEBLM LICENSE MANAGER INSTALLATION AND CONFIGURATION	9
5.1. INSTALL JAVA RUNTIME ENVIRONMENT.....	9
5.2. INSTALL APACHE TOMCAT.....	10
5.3. AVAYA WEBLM CONFIGURATION	14
6. ACCESSING WEBLM SERVER WEB PAGE	18
7. INSTALL LICENSE FILE	21
8. VERIFICATION STEPS.....	21
9. TROUBLESHOOTING	22
10. REFERENCES.....	24

1. Introduction

These Application Notes describe the steps for configuring the Avaya WebLM License Manager to support Avaya VPNremote™ Phones.

Avaya WebLM is a Web-based license manager that runs on both Microsoft Windows and UNIX systems. It is designed to support Avaya software products that require licensing. The WebLM server provides a Web User Interface (UI) for license administration which can be accessed from a standard web browser over a secure SSL link.

The Avaya VPNremote™ Phone is a software based Virtual Private Network (VPN) client integrated into the firmware of an Avaya IP Telephone. This enhancement allows the Avaya IP Telephone to be plugged in and used seamlessly over a secure VPN from any broadband Internet connection. The Avaya VPNremote Phone provides the identical telephony feature set and user experience as a standard Avaya IP Telephone offers in a typical office environment deployment. Avaya IP Telephone models supporting the Avaya VPNremote Phone firmware are the 4610SW, 4620SW, 4621SW, 4622SW and 4625SW.

Release 2 of the Avaya VPNremote Phone utilizes Avaya's WebLM license management system. A WebLM client application integrated into the Avaya VPNremote Phone communicates with the WebLM sever. The Avaya VPNremote Phone license file must be installed on the WebLM server for full functionality. The VPNremote Phone can function without a license file for a 30-day period. When the 30-day time period expires, the VPNremote Phone is non-operational and the user must install the previous firmware to the telephone for any functionality.

An Avaya sales representative or business partner must be contacted to obtain the VPNremote Phone license file.

1.1. Avaya VPNremote Phone Startup

The steps shown in **Figure 1** below describe the high level events that take place during the VPNremote phone startup process including access to the WebLM server.

1. The VPNremote Phone establishes an IPSec VPN tunnel upon boot up with the designated VPN gateway.
2. The VPNremote Phone initiates a TFTP or HTTP session with the phone configuration server (HTTP/TFTP Server) for configuration file download.
3. The VPNremote Phone initiates an HTTPS session with the WebLM server. The VPNremote Phone's WebLM client communicates with the WebLM server to request a license. The WebLM server verifies the request, confirms the license count will not be exceeded and grants a license.
4. The VPNremote Phone registers with Avaya Communication Manager and is ready for service.

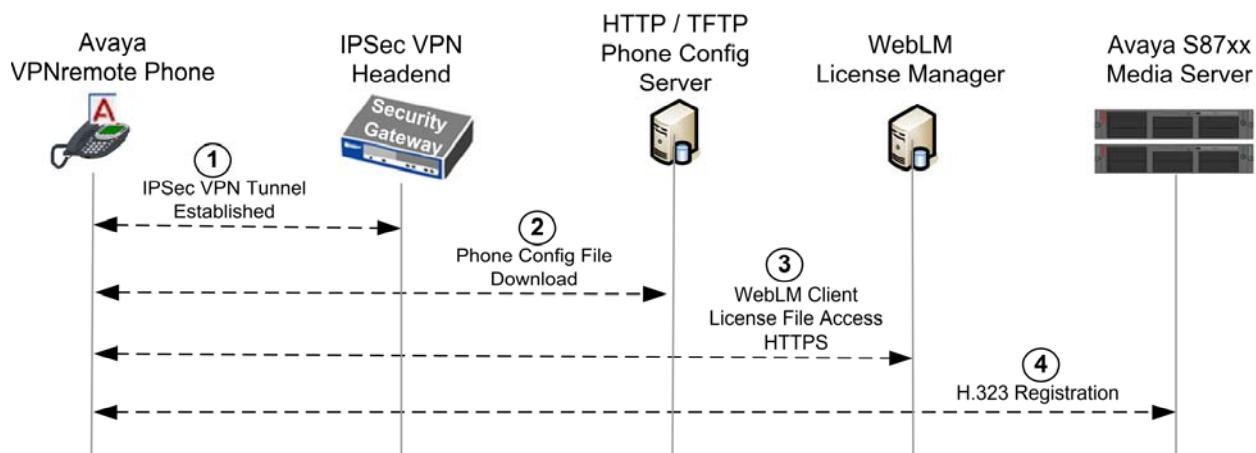


Figure 1: VPNremote Phone Startup

2. Network Topology

The sample network implemented for these Application Notes is shown in **Figure 2**. The WebLM License Manager supports both Linux and Windows platforms. Microsoft Windows 2000 Server was used in the sample configuration.

While separate physical servers are used for the WebLM License Manager and the HTTP/TFTP phone configuration download server in the sample network, they can be installed as co-resident applications on the same physical server.

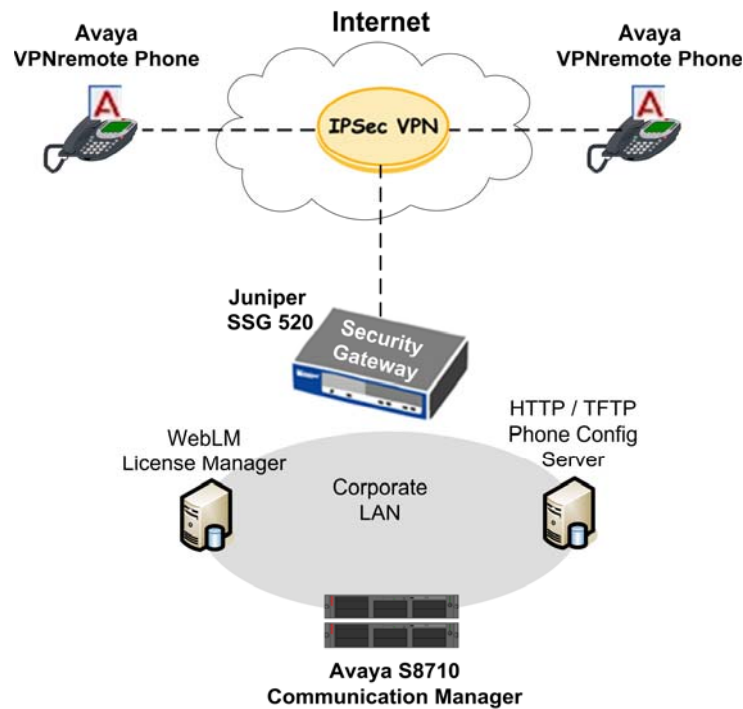


Figure 2: Network Topology

3. Equipment and Software Validated

Table 1 lists the equipment and software/firmware versions used in the sample configuration provided.

Component Description	Software/Hardware Version
Avaya S8710 Media Servers	Avaya Communication Manager R3.1.2 (R013x.01.2.632.1)
Avaya G650 Media Gateway IPSI (TN2312BP) C-LAN (TN799DP) MedPro (TN2302AP)	FW 022 (HW6) FW 016 (HW1) FW 108 (HW12)
Avaya 4610SW IP Telephones	R2.3 – Application (a10b VPN 232_1.bin)
Avaya 4620SW IP Telephones	R2.3 – Application (a20b VPN 232_1.bin)
Avaya 4621SW IP Telephones	R2.3 – Application (a20b VPN 232_1.bin)
Avaya 4625SW IP Telephones	R2.5 – Application (a25 VPN 252_1.bin)
Avaya WebLM License Manager	4.3
Apache Tomcat	5.5.17 – Core Distribution
Java Runtime Environment	Java 2 Standard Edition v1.5.0_8
Juniper Networks Secure Services Gateway 520	ScreenOS 5.4.0r1.0

Table 1 – Equipment and Software Validated

4. Avaya VPNremote Phone Configuration

4.1. VPNremote Phone Firmware

The Avaya VPNremote Phone firmware must be installed on the phone prior to the phone being deployed in the remote location. See **Section 10 References** *VPNremote for the 4600 Series IP Telephones Release 2.0 Administrator Guide* for details on installing the VPNremote Phone firmware. The firmware version of Avaya IP telephones can be identified by viewing the version displayed on the phone upon boot up or when the phone is operational by selecting the **Options** hard button → **View IP Settings** soft button → **Miscellaneous** soft button → **Right arrow** hard button. The Application file name displayed denotes the installed firmware version.

As displayed in **Table 1 – Equipment and Software Validated**, VPNremote Phone firmware includes the letters **VPN** in the file name. This allows for easy identification of firmware versions incorporating VPN capabilities.

4.2. Configuring Avaya VPNremote Phone

The VPNremote Phone configuration can be administered centrally from an HTTP or TFTP server or locally on the phone. See **Section 10 References** *VPNremote for the 4600 Series IP Telephones Release 2.0 Administrator Guide* for details on all the VPNremote Phone configuration parameters.

1. Locally Setting the Avaya VPNremote Phone File Server parameter

Most parameters of the **VPN Options** menu of the VPNremote Phone are VPN specific. The one parameter related to the WebLM server is the File Server parameter. As described in **Section 1.1 Figure 1**, the VPNremote Phone must first access the HTTP/TFTP file server which then identifies the location of the WebLM server through the configuration files downloaded to the VPNremote Phone. The File Server IP Address must be entered locally in the VPNremote Phone.

There are two methods available to access the **VPN Options** menu from the VPNremote Phone.

a. During Telephone Boot:

During the VPNremote Phone boot up, the option to press the * key to enter the local configuration mode appears on the telephone's display screen as shown below.

```
DHCP
* to program
```

When the * key is pressed, several configuration parameters are presented such as the phone's IP Address, the Call Server's IP Address, etc. Press the # key to accept the current settings or set to an appropriate value. The final configuration option displayed is the VPN Start Mode option shown below. Press the * key to enter the VPN Options menu.

```
VPN Start Mode: Boot
*=Modify  #=OK
```

b. During Telephone Operation:

While the VPNremote Phone is in an operational state (i.e. registered with Avaya Communication Manager) press the following key sequence on the telephone to enter VPN configuration mode:

Mute-V-P-N-M-O-D-# (Mute-8-7-6-6-6-3-#)

The follow is displayed:

```
VPN Start Mode: Boot
*=Modify  #=OK
```

Press the * key to enter the **VPN Options** menu.

2. Setting the NVWEBLMURL Variable

One of the configuration script files downloaded by the VPNremote Phone from the HTTP/TFTP file server is the 46VPNsetting.txt file. The 46VPNsetting.txt file contains many variables including the variable **NVWEBLMURL** which identifies all available WebLM servers to the VPNremote Phone. Below are the specifics of the **NVWEBLMURL** variable:

- Variable Name: **NVWEBLMURL**
- Valid Values:
 - Comma separated URLs of available WebLM Licensing servers.
 - Length of individual URL cannot be more than 128 characters.
 - Combined length of all the URLs cannot be more than 252 characters.
 - Default URL of the WebLM Licensing Server is:

http://xxx.xxx.xxx.xxx:8080/WebLM/LicenseServer

Where xxx.xxx.xxx.xxx is the IP address (or FQDN) of the WebLM server.

- Example:
 - SET NVWEBLMURL http://192.168.1.30:8080/WebLM/LicenseServer

5. Avaya WebLM License Manager Installation and Configuration

5.1. Install the Java Runtime Environment

The Avaya WebLM application, when installed on a Microsoft Windows platform, requires both the **Java Runtime Environment (JRE)** and **Apache Tomcat** applications be installed on the system to be used for WebLM. See **Table 1** for versions used for these Application Notes. The JRE must be installed first followed by Apache Tomcat. Default settings were chosen during installation for both applications.

1. Download JRE

The following link is to the Sun Java download web site to access the J2RE 5.0 Update 8 used for these Application Notes.

<https://sdlc1a.sun.com/ECom/EComActionServlet;jsessionid=DF5A17809CDF026408A3AFDC62555E14>

2. Install JRE

Execute the downloaded J2SE 5.0 installation script and follow the prompts.

3. Verify JRE

Verify the installation by going to **Windows Control Panel > Add/Remove Programs**. J2SE Runtime Environment 5.0 Update 8 should be displayed in the **Currently Installed Programs** list.



5.2. Install Apache Tomcat

With the JRE application installed from **Section 5.1**, download and install the Apache Tomcat for Windows server application.

1. Download Apache Tomcat

The following URL is to the Apache Tomcat download web site to access the Tomcat server version 5.5.17 used for these Application Notes.

<http://tomcat.apache.org/download-55.cgi#5.5.17>

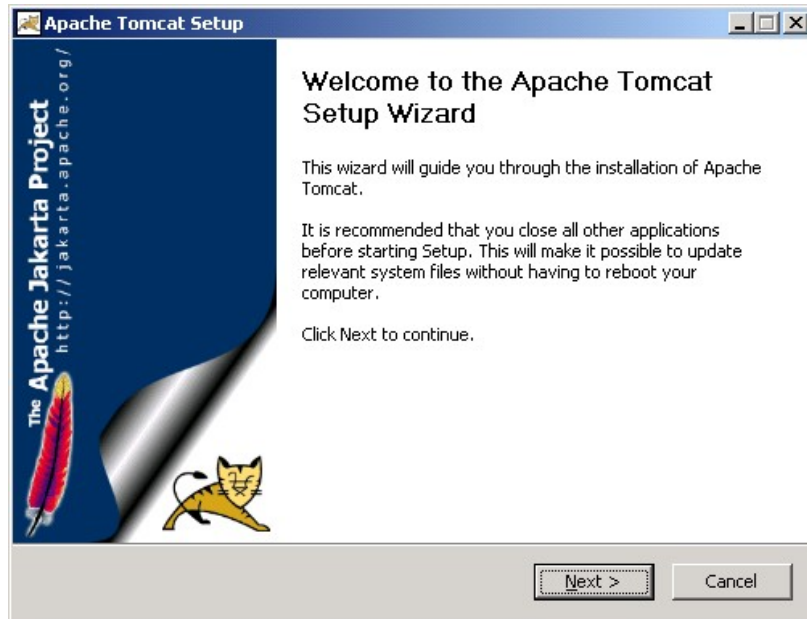
From the download web page select ○ **Windows Executable (pgp, md5)**
under **Core** distribution, as shown below.

Binary Distributions

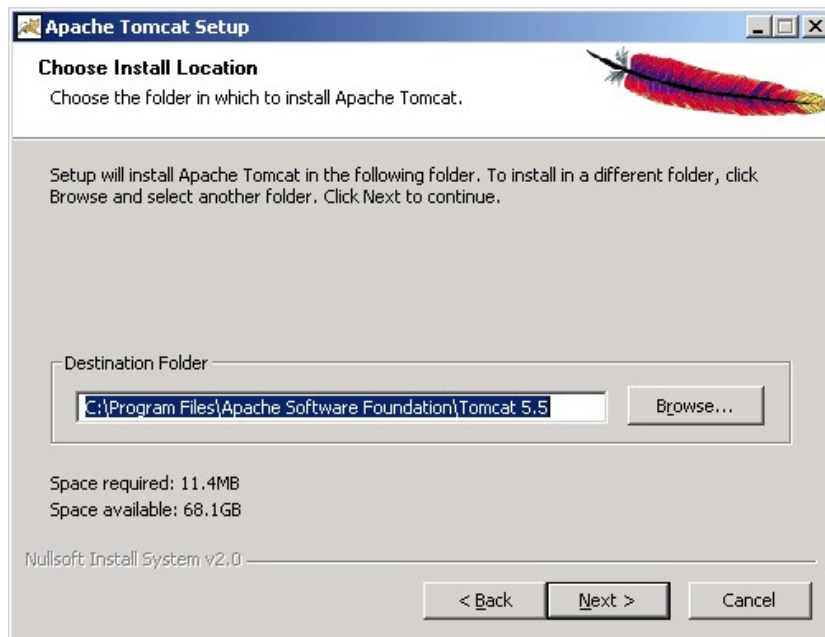
- Core:
 - [zip](#) ([pgp](#), [md5](#))
 - [tar.gz](#) ([pgp](#), [md5](#))
 - [Windows Executable](#) ([pgp](#), [md5](#))
- Deployer:
 - [zip](#) ([pgp](#), [md5](#))
 - [tar.gz](#) ([pgp](#), [md5](#))
- Embedded:
 - [zip](#) ([pgp](#), [md5](#))
 - [tar.gz](#) ([pgp](#), [md5](#))
- Administration Web Application:
 - [zip](#) ([pgp](#), [md5](#))
 - [tar.gz](#) ([pgp](#), [md5](#))
- JDK 1.4 Compatability Package:
 - [zip](#) ([pgp](#), [md5](#))
 - [tar.gz](#) ([pgp](#), [md5](#))
- Documentation (Already Included in Core Downloads):
 - [tar.gz](#) ([pgp](#), [md5](#))

2. Install Apache Tomcat

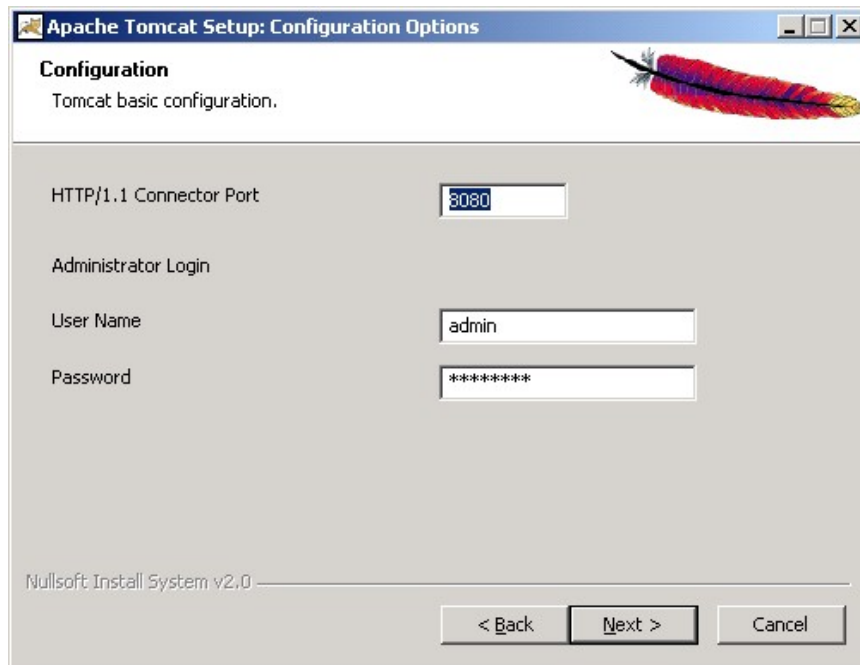
Execute the downloaded Apache Tomcat 5.5.17 installation script and follow the prompts. Below are a few of the screens that appear during the Tomcat installation which require input. The first screen to appear to start the installation is shown below.



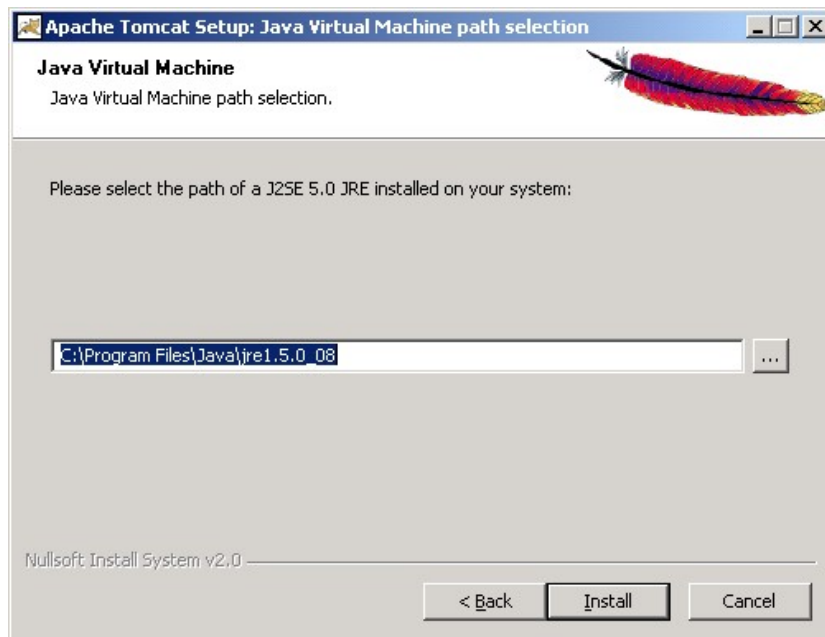
Note the Destination Folder used for the Tomcat installation. This folder path is needed in **Section 5.3** of these Application Notes.



Note the HTTP Port number Tomcat will run under. This port number is need when accessing the URL for WebLM described in **Section 6** of these Application Notes.

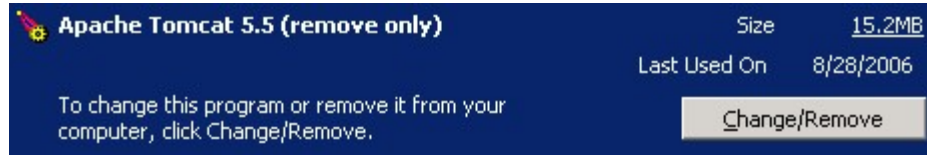


The Java Runtime Environment application installed in **Section 5.1** is shown on the following screen.




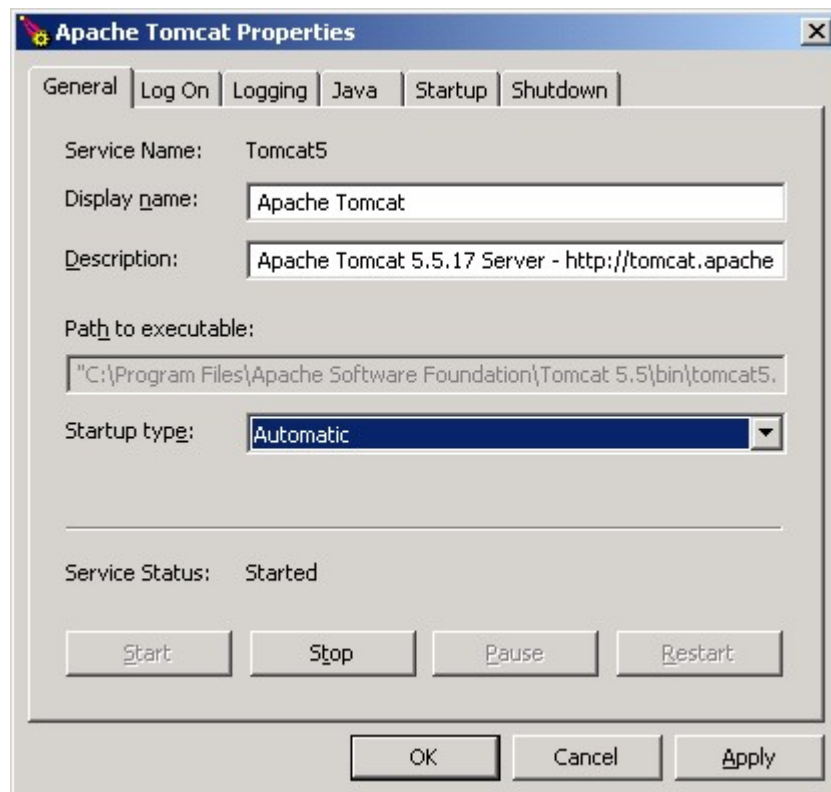
3. Verify Apache Tomcat

Verify the installation by going to **Windows Control Panel → Add/Remove Programs**. Apache Tomcat 5.5 should be displayed in the **Currently Installed Programs** list.



4. Set Tomcat Startup Type

The Apache Tomcat server icon  appears in the bottom right corner of the Windows toolbar. Select this icon for additional Apache Tomcat configuration options. Apache Tomcat runs as a Windows service which defaults to a startup type of manual. It is recommended to change the startup type to Automatic to ensure Apache Tomcat starts when Windows restarts.



5.3. Avaya WebLM Configuration

The steps below describe the installation and configuration of the Avaya WebLM License Manager running in a Microsoft Windows environment. The installation is a manual process and requires copying, moving and editing files. Refer to the WebLM release notes prior to installation. The following areas are covered:

- **Download and Extract WebLM files**
- **Copy WebLM Files**
- **Extract Contents of WebLM.war to the WebLM Folder**
- **Enabling HTTPS**

1. Download and Extract WebLM files

The WebLM software and release notes may be downloaded from the Avaya support web site. From a web browser, navigate to the following links or enter the URL shown below to go directly to **VPNremote Telephone Download** page.

<http://support.avaya.com> → **FIND DOCUMENTATION and TECHNICAL INFORMATION by PRODUCT NAME** → **VPNremote™ Phone** → **Downloads** → **VPNremote Telephone Download**

<http://support.avaya.com/japple/css/japple?temp.documentID=286394&temp.productID=280576&temp.releaseID=280577&temp.bucketID=108025&PAGE=Document>

The **WebLM download (Windows)** option from the above link was used for these Application Notes.

AVAYA United States | Worldwide [Contacts](#) | [Support](#) [Advanced Search](#)

IP Telephony **Contact Centers** **Mobility** **Services**

[Support > VPNremote™ Phone >](#)
VPNremote™ Phone: Downloads

VPNremote™ Phone: Downloads
▶ Administration and System Programming Downloads
▶ Installation, Migrations, Upgrades and Configurations
▶ [View all documents](#)

Find another product

Release 2.3.2 | Select a release [▶](#)

[◀ Back](#)

VPNremote Telephone Download

VPNremote Phone allows for secure remote IP telephony access through a Security Gateway. This software will convert a standard H323 IP telephone 4610SW, 4620SW, 4621SW, 4622SW and 4625SW to a VPNremote Phone.

[VPNremote Phone readme](#)

[English - VPNremote Phone Download](#)
Download file size is 17 MB.

[Chinese-Russian - VPNremote Phone Download](#)
Download file size is 17.3 MB.

[Japanese-Russian - VPNremote Phone Download](#)
Download file size is 17.3 MB.

VPNremote Phone requires WebLM Licensing. The WebLM software and release notes may be downloaded from the links below.

[WebLM Readme](#)

[WebLM Download \(Windows\)](#)
Download file size is 1.4 MB.

[WebLM Download \(Other\)](#)
Download file size is 1.4 MB.

Connect with Avaya

Contact Support:
▶ [Support Directory](#)
▶ [Escalation Contacts](#)

Online Service Manager

▶ [Create Service Request](#)
▶ [Check Case Status](#)
▶ [Parts Replacement](#)
▶ [My E-Notifications](#)
▶ [New User Registration](#)
▶ [Help](#)

Administration

▶ [Sold To Administration](#)
▶ [Site Contacts](#)

Related Services

▶ [Download Center/FAQ](#)
▶ [Online Expert](#)
▶ [OtelAccess License Key](#)
▶ [My Sites](#)
▶ [Avaya Web Ticketing \(non-US only\)](#)
▶ [Avaya Global eBill Tutorial](#)

The WebLM software download is in the form of a zip file. Unzip the WebLM_Windows.zip file to the PC where WebLM will be installed.

The following files are extracted:

- **WebLM.war:** A **.war** file, short for **Web Archive**, is a compressed ZIP file used to distribute a set of Java classes. The WebLM.war file contains core WebLM files providing the primary WebLM functionality and licensing server components.
- **mail.jar:** Required by the WebLM server to send email to the administrator.
- **activation.jar:** Used internally by mail.jar.

2. Copy WebLM files

The extracted files from **Step 1** above must now be copied to designated directories under the Apache Tomcat server as shown below.

- Copy **WebLM.war** to the *<tomcat_installed_dir>\webapps* directory
(*i.e.* C:\Program Files\Apache Software Foundation\Tomcat 5.5\webapps).
- Copy **mail.jar** to the *<tomcat_installed_dir>\common\lib* directory
(*i.e.* C:\Program Files\Apache Software Foundation\Tomcat 5.5\common\lib).
- Copy **activation.jar** to the *<tomcat_installed_dir>\common\lib* directory
(*i.e.* C:\Program Files\Apache Software Foundation\Tomcat 5.5\common\lib).

3. Extract Contents of WebLM.war to the WebLM Folder

- Create a folder named **WebLM** under the *<tomcat_installed_dir>\webapps* directory.
(*i.e.* C:\Program Files\Apache Software Foundation\Tomcat\5.5\webapps).
- Open the **WebLM.war** file using the Windows Zip (WinZIP) application and extract the contents of **WebLM.war** to the WebLM directory.

4. Enable HTTPS

It is recommended the Tomcat server be configured for HTTPS to ensure secure communications with the WebLM application. The following steps configure Tomcat for HTTPS when accessing the WebLM application.

Note: Refer to the section titled “SSL Config HOW TO” in the Tomcat 5 documentation for more detailed instructions.

- Using a text editor such as Windows Notepad, edit the file **server.xml** located in `<tomcat_installed_dir>\conf` (i.e. `C:\Program Files\Apache Software Foundation\Tomcat\5.5\conf`)
- Search for the following text:

<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->

The text below shows a “**before edit**” view of the HTTPS <Connector>.

Prior to server.xml edit:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
    <Connector port="8443" maxHttpHeaderSize="8192"
        maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
        enableLookups="false" disableUploadTimeout="true"
        acceptCount="100" scheme="https" secure="true"
        clientAuth="false" sslProtocol="TLS" />
-->
```

- Uncomment this entire HTTPS <Connector> tag by removing the tag **<!--** before the start of **<Connector port="8443"**. Also remove the tag **-->** after the end of the <Connector> tag.

- The last line of this HTTPS <Connector> tag contains the following line:
`clientAuth="false" sslProtocol="TLS" />`

Add the following three attributes to the end of the HTTPS <Connector> tag in front of the />:

```
keystoreFile="./webapps/WebLM/WEB-INF/weblmserver.p12"
keystoreType="PKCS12"
keystorePass="weblmserver"
```

The text below shows an “**after edit**” view of the HTTPS <Connector>. Save the server.xml file when edits are complete.

After server.xml edit:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->

<Connector port="8443" maxHttpHeaderSize="8192"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false" disableUploadTimeout="true"
    acceptCount="100" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS"
    keystoreFile="./webapps/WebLM/WEB-INF/weblmserver.p12"
    keystoreType="PKCS12" keystorePass="weblmserver" />
```

- **Restart Tomcat:** The Windows Tomcat service must be stopped and restarted for the changes to server.xml to take effect and enable HTTPS.

6. Accessing WebLM Server Web Page

1. Enter WebLM Server URL

From a web browser, enter the URL of the WebLM server,
(i.e. **http://<WebLM Server IP address>:8080/WebLM/index.jsp**)

The following URL is used for these Application Notes:
http://192.168.1.30:8080/WebLM/index.jsp

A security alert popup window appears informing the user that communication between the web browser and WebLM server will be transferred over the secured network connection. The user is required to accept the security alert.

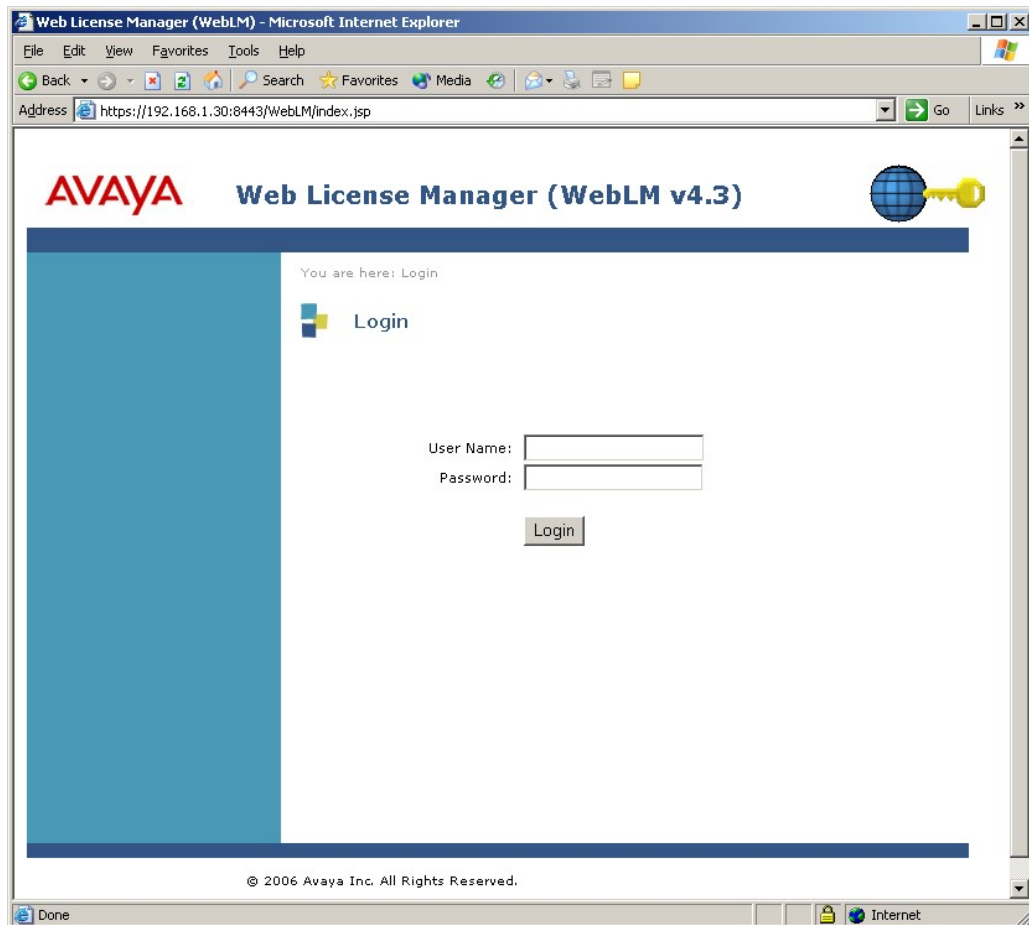


The web browser will then be automatically redirected to **https://WebLM Server IP address:8443/WebLM/index.jsp**. Note the change in the URL from http to https and the port number change from 8080 to 8443.

From this point, all communication between the web browser and the WebLM server will be over the secure HTTPS connection.

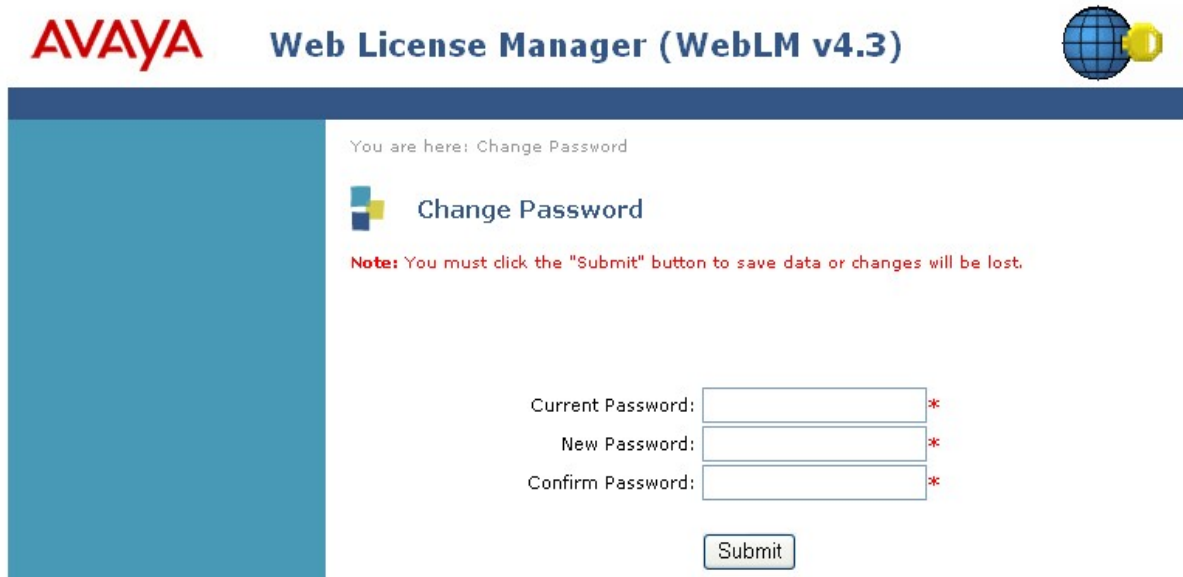
2. WebLM Server Log in

The WebLM login web page, similar to the one below, appears. For the first time logging into WebLM, enter the username of “**admin**” and a password of “**weblmadmin**”.



3. WebLM Server Forced Password Change


For the first time log in, the user (admin) will be forced to change the password. Only after the password is changed can the user move ahead. Once the password is changed, the user will be logged out automatically and required to log in with the new password.



The screenshot shows the Avaya Web License Manager (WebLM v4.3) interface. At the top, the Avaya logo is on the left, the title "Web License Manager (WebLM v4.3)" is in the center, and a globe icon with a yellow key is on the right. Below the title bar, a blue sidebar is on the left. The main content area has a breadcrumb "You are here: Change Password" and a heading "Change Password" with a small icon. A red note states: "Note: You must click the 'Submit' button to save data or changes will be lost." Below this, there are three input fields labeled "Current Password:", "New Password:", and "Confirm Password:", each followed by a red asterisk. A "Submit" button is located below the input fields.

AVAYA Web License Manager (WebLM v4.3)

You are here: Change Password

 Change Password

Note: You must click the "Submit" button to save data or changes will be lost.

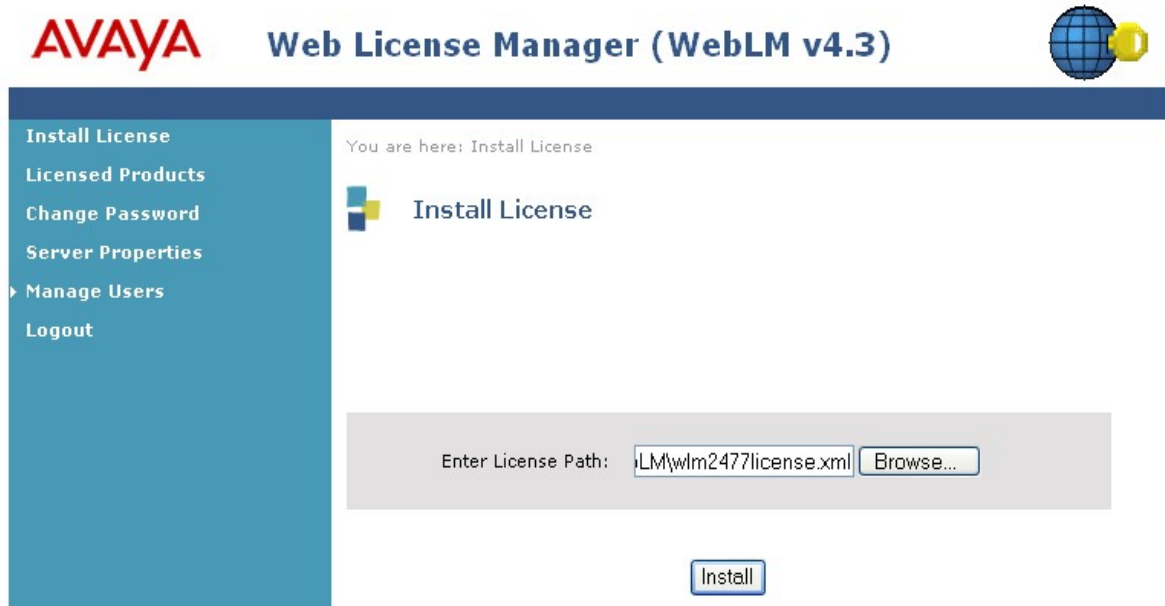
Current Password: *

New Password: *

Confirm Password: *

7. Install License File

The VPNremote Phone license file can now be uploaded to the WebLM license server. Copy the VPNremote Phone license file to a directory on the WebLM Server. From the WebLM Server Administration Web UI, select **Install License** from the left navigation menu to display the Install License page. From the Install License page, select **Browse** to navigate to the VPNremote Phone license file. Select **Install** to upload the license file to the WebLM server.



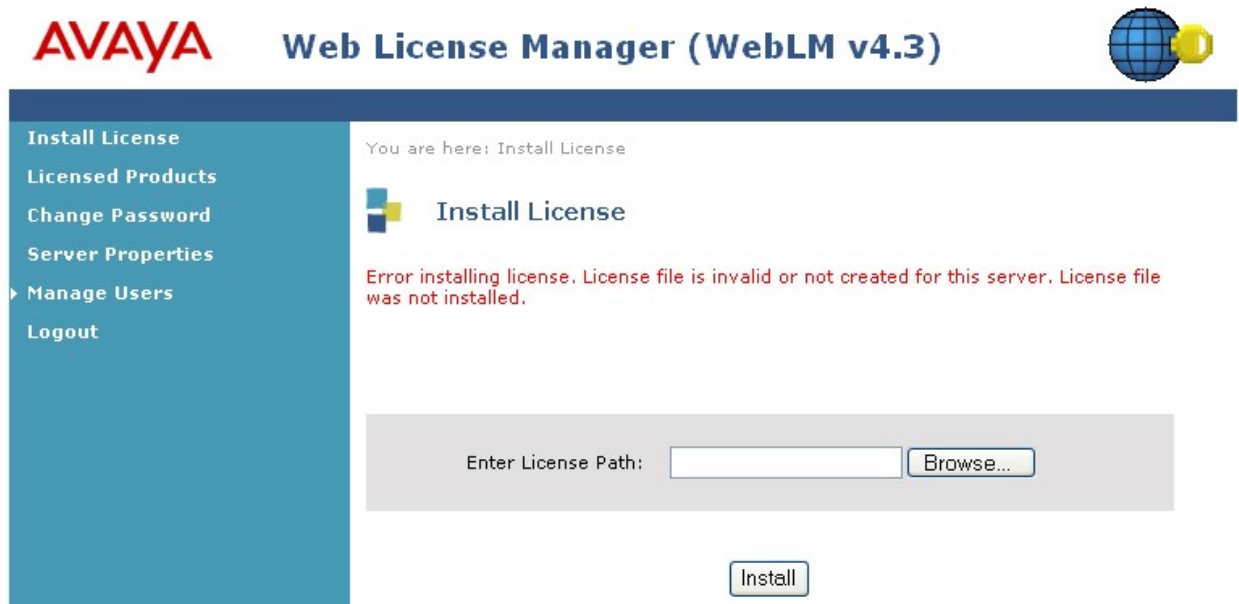
8. Verification Steps

The VPNremote Phone displays a WebLM client successful message when the WebLM server is successfully contacted during the phone boot up process. This indicates a valid license has been reserved for the VPNremote Phone.

9. Troubleshooting

1. License File Error

The following error message is displayed if the license file is not successfully installed in the WebLM server. License files are created for specific WebLM Servers based on the WebLM Servers primary NIC MAC address. The error displayed below is the result of an attempt to install a license file on a WebLM Server with a MAC address that did not match the one the license file expected. For additional information see **License File Upload Error:** in **Step 2** below. Contact an Avaya sales representative or business partner for assistance.



2. WebLM Logs

The WebLM Server maintains an active log of events. The log file, **weblmserver.log**, can be found in the following directory *<tomcat_installed_dir>\webapps\WebLM\data\log* .

(i.e. *C:\Program Files\Apache Software Foundation\Tomcat 5.5\webapps\WebLM\data\log\weblmserver.log*)

Below are some examples of a WebLM Server log:

- **First Time Web UI login:**

```
INFO WebLMUI - Remote user: - Login request. WebLM user name: admin
INFO WebLMUI - Remote user: - WebLM user admin logged in for the first
                        time. Transfer to set password page.
INFO WebLMUI - Remote user: - WebLM user: admin requests password change.
INFO WebLMUI - Remote user: - WebLM user admin session has been invalidated
INFO WebLMUI - Remote user: - Login request. WebLM user name: admin
INFO WebLMUI - Remote user: - WebLM user admin logged in
```

- **License File Upload:**

```
INFO WebLMUI - Remote user: - WebLM user: admin requesting license install.
INFO WebLM    - Name of uploaded License File is wlm2477license.xml
```

- **License File Upload Error:**

```
ERROR com.avaya.weblm.b.c - Host id mismatch. Host Id from WebLM server:
                        000CF1E76DB8.
ERROR WebLMlib - License file contain invalid product(getting null)
ERROR Exception - Error= Error Code = 32, Message = 'License file is invalid
                        or not created for this server. License file was
                        not installed.'
```

3. Apache Tomcat Logs

The Apache Tomcat Server maintains several active log files which can be found in the following default directory: *<tomcat_installed_dir>\logs*

(i.e. *C:\Program Files\Apache Software Foundation\Tomcat 5.5\logs*)

10. Conclusion

The Avaya WebLM application provides a secure, easy to use tool for the management of licenses required by Avaya products including the Avaya VPNremote Phone.

11. References

1. Avaya VPNremote Phone and WebLM Server software download
<http://support.avaya.com/japple/css/japple?temp.documentID=286394&temp.productID=280576&temp.releaseID=280577&temp.bucketID=108025&PAGE=Document>
2. Avaya VPNremote for the 4600 Series IP Telephones Release 2.0 Administrator Guide
<http://support.avaya.com/japple/css/japple?temp.documentID=292326&temp.productID=280576&temp.releaseID=280577&temp.bucketID=159898&PAGE=Document>
3. Avaya VPNremote Phone documentation
<http://support.avaya.com/japple/css/japple?PAGE=ProductArea&temp.productID=280576&temp.releaseID=280577>
4. Avaya Administrators Guide for Communication Manager
http://support.avaya.com/elmodocs2/comm_mgr/r3/pdfs/03_300509_1.pdf
5. Java Runtime Environment
<http://www.java.com/en/download/manual.jsp>
6. Apache Tomcat
<http://tomcat.apache.org/index.html>
7. Additional Avaya Application Notes and Resources are available,
<http://www.avaya.com/gcm/master-usa/en-us/resource/>

©2006 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com